

Application No. 10800983 (Docket: CNTR.2073)  
37 CFR 1.111 Amendment dated 06/21/2007  
Reply to Office Action of 03/21/2007

RECEIVED  
CENTRAL FAX CENTER  
JUN 21 2007

### AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

#### SUMMARY OF THE INVENTION

[0020.1] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes an instruction register having a cryptographic instruction disposed therein~~cryptographic instruction~~, keygen logic~~and execution logic~~, a keygen unit, and an execution unit. The cryptographic instruction is received by a computing device~~microprocessor~~ as part of an instruction flow executing on the computing device~~microprocessor~~. The cryptographic instruction prescribes one of the cryptographic operations, and also prescribes that a user-generated key schedule be employed when executing the one of the cryptographic operations. The keygen unit~~keygen logic~~ is operatively coupled to the cryptographic instruction register. The keygen unit~~keygen logic~~ directs the computing device~~microprocessor~~ to load the user-generated key schedule. The ~~execution logic~~ execution unit is operatively coupled to the keygen unit~~keygen logic~~. The ~~execution logic~~ execution unit employs the user-generated key schedule to execute the one of the cryptographic operations. The execution unit includes a cryptography unit that is configured execute a plurality of cryptographic rounds on each of the plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, where the plurality of cryptographic rounds are prescribed by a control word that is provided to the cryptography unit.

[0021] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has a cryptography unit within a device~~microprocessor~~ and keygen logic~~keygen unit~~. The cryptography unit executes one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes the one of the cryptographic operations. The

Application No. 10800983 (Docket: CNTR.2073)  
37 CFR 1.111 Amendment dated 06/21/2007  
Reply to Office Action of 03/21/2007

cryptographic instruction also prescribes that a user-generated key schedule be employed when executing the one of the cryptographic operations. The ~~keygen-logic~~keygen unit is operatively coupled to the cryptography unit. The ~~keygen-logic~~keygen unit directs the ~~device-microprocessor~~ to perform the one of the cryptographic operations and to employ the user-generated key schedule when performing the one of the cryptographic operations.

[0022] Another aspect of the present invention provides a method for performing cryptographic operations in a ~~device~~microprocessor. The method includes receiving a cryptographic instruction from memory that prescribes employment of a user-generated key schedule during execution of one of a plurality of cryptographic operations and within a cryptographic unit in the microprocessor, employing the user-generated key schedule when executing the one of the cryptographic operations to generate a result of the one of the cryptographic operations, employing the user-generated key schedule when executing the one of the cryptographic operations.